(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
29. August 2002 (29.08.2002)

PCT

(10) Internationale Veröffentlichungsnummer
WO 02/067108 A2

(51) Internationale Patentklassifikation[7]: G06F 7/72

(21) Internationales Aktenzeichen: PCT/EP02/00719

(22) Internationales Anmeldedatum:
24. Januar 2002 (24.01.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 07 376.3 16. Februar 2001 (16.02.2001) DE

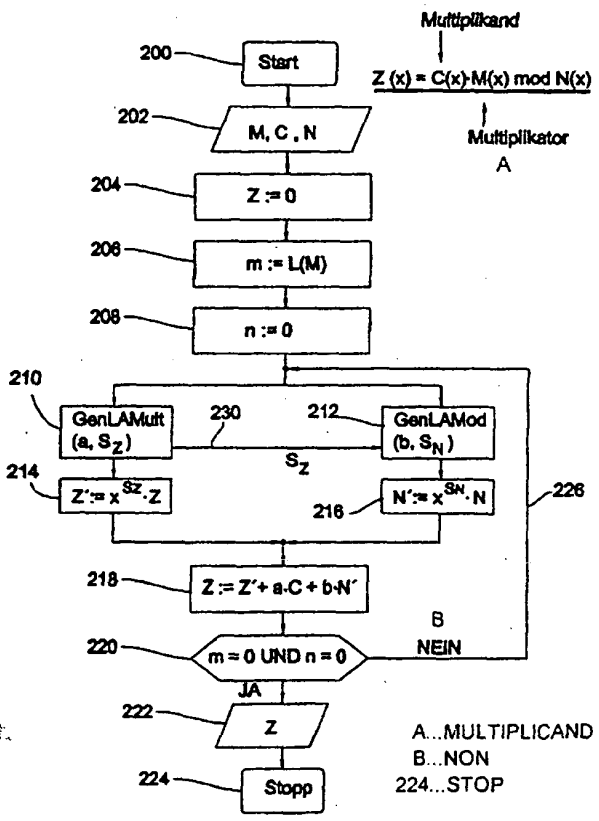
(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **INFINEON TECHNOLOGIES AG** [DE/DE]; St.-Martin-Str. 53, 81669 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **ELBE, Astrid** [DE/DE]; Salzmesserstr. 41, 81829 Muenchen (DE). **SEDLAK, Holger** [DE/DE]; Neumuenster 10a, 85658 Egmating (DE). **JANSSEN, Norbert** [DE/DE]; Innere-Wiener-Str. 13a, 81667 Muenchen (DE). **SEIFERT, Jean-Pierre** [DE/DE]; Harsdoerfer Str. 1, 81669 Muenchen (DE).

[Fortsetzung auf der nächsten Seite]

(54) **Title:** METHOD AND DEVICE FOR CONDUCTING MODULAR MULTIPLICATION AND ARITHMETIC-LOGIC UNIT FOR CONDUCTING MODULAR MULTIPLICATION

(54) **Bezeichnung:** VERFAHREN UND VORRICHTUNG ZUM MODULAREN MULTIPLIZIEREN UND RECHENWERK ZUM MODULAREN MULTIPLIZIEREN



(57) **Abstract:** According to a method for conducting modular multiplication of a multiplicand (C) with a multiplier (M) while using a module (N), whereby the multiplicand, the multiplier and the module are polynomials of a variable, a multiplication forecast method (210) is executed in order to obtain a multiplication shift value (s_Z). An intermediate result polynomial (Z) is shifted (214) leftward by the number of places of the multiplication shift value (s_Z) in order to obtain a shifted intermediate result polynomial (Z'). In addition, a reduction forecast method (212) is executed in order to obtain a reduction shift value (s_N), whereby the reduction shift value is equal to the difference of the degree of the shifted intermediate result polynomial (Z') and of the degree of the module polynomial (N). The module polynomial is shifted by a number of places equal to the reduction shift value (216) in order to obtain a shifted module polynomial. In a three-operand addition (218), the shifted intermediate result polynomial (Z') and the multiplicand (C) are added, and the shifted module polynomial (N') is subtracted in order to obtain an updated intermediate result polynomial (Z). By iteratively executing (226) the above-mentioned steps, the modular multiplication is gradually carried out until all the powers of the multiplier polynomial are processed. A transfer-interrupt function makes it possible to carry out both a Z/NZ arithmetic as well as a GF(2^n) arithmetic on a single long number arithmetic-logic unit.

[Fortsetzung auf der nächsten Seite]

WO 02/067108 A2

(74) **Anwälte:** **SCHOPPE, Fritz** usw.; Schoppe, Zimmermann, Stöckeler & Zinkler, Postfach 71 08 67, 81458 München (DE).

(81) **Bestimmungsstaaten** *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) **Bestimmungsstaaten** *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Docket # SAZIO 020103

Applic. #

Applicant: Ashid Elbeelal.

Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100 Fax: (954) 925-1101

(57) Zusammenfassung: Verfahren und Vorrichtung zum modularen Multiplizieren und Rechenwerk zum modularen Multiplizieren Bei einem Verfahren zum modularen Multiplizieren eines Multi-plikanden (C) mit einem Multiplikator (M) unter Verwendung eines Moduls (N), wobei der Multiplikand, der Multiplikator und der Modul Polynome einer Variablen sind, wird ein Multi-plikations-Vorausschau-Verfahren (210), um einen Multiplika-tions-Verschiebungswert (sZ) zu erhalten, ausgeführt. Ein Zwischenergebnis-Polynom (Z) wird um die Anzahl von Stellen des Multiplikations-Verschiebungs-Werts (sZ) nach links ver-schoben (214), um ein verschobenes Zwischenergebnis-Polynom (Z') zu erhalten. Darüber hinaus wird ein Reduktions-Vorausschau-Verfahren (212), um einen Reduktions-Verschiebungswert (sN) zu erhalten, ausgeführt, wobei der Re-duktions-Verschiebungswert gleich der Differenz des Grads des verschobenen Zwischenergebnis-Polynoms (Z') und des Grads des Modul-Polynoms (N) ist. Hierauf wird das Modul-Polynom um ei-ne Anzahl von Stellen gleich dem Reduktions-Verschiebungswert verschoben (216), um ein verschobenes Modul-Polynom zu erhal-ten. In einer Drei-Operanden-Addition (218) werden das ver-schobene Zwischenergebnis-Polynom (Z') und der Multiplikand (C) summiert, und das verschobene Modul-Polynom (N') wird subtrahiert, um ein aktualisiertes Zwischenergebnis-Polynom (Z) zu erhalten. Durch iteratives Ausführen (226) der vorste-henden Schritte wird die modulare Multiplikation nach und nach abgearbeitet, bis sämtliche Potenzen des Multiplikator-Polynoms verarbeitet sind. Durch eine Übertrag-Abschalt-Funktion ist es möglich, sowohl eine Z/NZ-Arithmetik als auch eine GF(2n)-Arithmetik auf einem einzigen Langzahl-Rechenwerk auszuführen.